5 FAM 790
USING SOCIAL MEDIA

(CT:IM-110; 06-10-2010)
(Office of Origin: IRM/BMP/GRP)

5 FAM 791 SCOPE

(CT:IM-110; 06-10-2010)

a. Social media consist of a variety of digital technologies that foster interaction among individuals who use the tools. Social media enable individuals to post their own content to Web sites accessible to others; comment on, rate and/or tag content that others have posted; download distributed media files; dynamically develop software applications; interact in simulated learning, gaming and trading environments; engage in online conversations; and observe the interactions of others.

b. Social media provide an important means for the Department to fulfill its lead role in conduct of U.S. foreign policy. This subchapter provides guidance for accessing and using social media to:

   (1) Conduct internal and external collaboration within State and between the Department and other Federal Government agencies;

   (2) Conduct diplomatic activities with non-U.S. Government organizations and individuals on controlled-access Web sites that are not available to the general public;

   (3) Use for official consular, public affairs and public diplomacy activities on Web sites that are available to the general public; and

   (4) (Use for engaging in activities that are of official concern to the Department.

The provisions of this subchapter apply to all Department personnel and all users of Department systems, including Foreign Service (FS) employees, Civil Service (CS) employees, employees abroad including locally employed staff (LE staff), and contractors performing duties under their contract with the Department of State.

5 FAM 791.1 Authorities

(CT:IM-110; 06-10-2010)

The following authorities are in addition to those listed in 5 FAM 712:

(1) Executive Order 13526, Classified National Security Information, or subsequent orders;

(2) Safeguarding Personally Identifiable Information, M-06-15 (May 22, 2006);

(3) Protection of Sensitive Agency Information, M-06-16 (June 23, 2006)

(4) Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, M-06-19 (July 12, 2006);

(5) Memorandum: Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006)

(6) Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16 (May 22, 2007)

(7) New FISMA Privacy Reporting Requirements for FY 2008, M-08-09 (January 18, 2008)

(8) The Digital Millennium Copyright Act, P.L. 105-304

(9) The Federal Advisory Committee Act, P.L. 92-463, Section 1

(10) The Hatch Act, 5 U.S.C. 7321-7326

(11) The Anti-Deficiency Act, 31 U.S.C. 1341 et seq. and 31 U.S.C. 1511 et seq.

(12) The Federal Tort Claims Act, 28 U.S.C. 1346(b), 1402(b), 2401(b), 2671-2680

(13) Federal Records Act, 44 U.S.C. 2108 and 44 U.S.C. 31, Records Management by Federal Agencies

(14) 5 C.F.R. 2635, Standards of Ethical Conduct for Employees of the Executive Branch

(15) 5 C.F.R. 734, Political Activities of Federal Employees

(16) 3 FAM 4120, Employee Responsibilities Abroad

(17) 3 FAM 4123, Restrictions on Employment and Outside Activities

(18) 3 FAM 4125, Outside Employment and Activities by Spouses and Family Members Abroad

(19) 3 FAM 4126, Outside Employment and Activities of Non-U.S. Citizen Employees and Locally-hired U.S. Citizen Employees

(20) 3 FAM 4170, Official Clearance of Speaking, Writing, and Teaching

(21) 5 FAM 460, Privacy Act Requirements

(22) 5 FAM 490, Use of Copyrighted Material

(23) 5 FAM 400, Records Management Requirements

(24) 5 FAM 700, Internet and Intranet Use

(25) Use of Department and Government Seals; 18 U.S.C. 713 and 1017

(26) The Anti-Lobbying Act, 18 U.S.C. 1913

(27) OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites

5 FAM 791.2 Additional Subchapter Definitions

(CT:IM-110; 06-10-2010)

The definitions presented for purposes of this FAM subchapter are in addition to those found in 5 FAM 713; 5 FAM 415; and 5 FAM 613.

Branding: Using graphics such as the Department seal, and other descriptive terminology, that marks a public site as an official site of the Department of State.

Department personnel: This term refers to Department of State employees, including Foreign Service (FS) employees, Civil Service (CS) employees, employees abroad, including locally employed staff (LE staff), and contractors (including personal service contractors) performing duties under their contract with the Department of State.

Nonrecord material: As it pertains to social media, site content that duplicates information in other Department Websites would be considered nonrecord material.

Privacy policy: A statement made by an organization regarding why, how, and pursuant to what legal authority (if applicable) personal data is being collected at a public Web site or social media site, and how the owner of the site will use any information obtained.

Public site: An Internet site that is available without restriction to a broad, undefined non-Government public audience. Social media or Web sites on closed U.S. Government networks of the Department or other U.S. Government entities are not considered public sites.

Site administrator: The individual who exercises day-to-day responsibility for managing content on a social media site. This person may also have responsibility for technical administration of the site.

Site sponsor: The organization that provides resources for Department of State social media sites.

Social media: Digital technologies and platforms that allow publishing, communication, and collaboration among individuals and institutions.

Social media applications: Web-based, specialized, sets of code and content that plug into social networks or other forms of social media,

allowing for greater sharing and dissemination of information. Examples are:

(1) Gadgets and widgets: Simplified, coded applications that are used to present information from or interact with more robust applications; and

(2) APIs (application programming interfaces): The modules of source code with business layer logic that developers use to interact with robust social media applications.

Social networks: Online communities that enable people to locate and connect with others, publicize and share their personal or professional networks, and establish, sustain and expand relationships. Social networks can be broad-based or topically and demographically specific.

Terms of Service: A contract between a service or platform provider and the Department of State regarding the user of that service or platform.

Terms of use: An agreement between the user of a State Department social media site and the Department.

5 FAM 792 SOCIAL MEDIA ENVIRONMENTS AND USE

(CT:IM-110; 06-10-2010)

Social media are approved for official use on unclassified and classified Department intranets and extranets, unclassified and classified U.S. Government interagency networks, and the Internet subject to the limitations and prohibitions outlined in 5 FAM 790. (See 5 FAM 796 for limitations on social media software installation on OpenNet and ClassNet.) Department social media sites may be open to all users of the network or closed except to a defined set of users on the network. Personnel may use social media on unclassified systems in a personal capacity, in accordance with 5 FAM 723.

5 FAM 792.1 Access To and Use of Social Media

(CT:IM-110; 06-10-2010)

a. As a general matter, the Department encourages the responsible use of social media consistent with current laws, policies and guidance that govern information and information technology. Department organizations will not arbitrarily ban access to or the use of social media.

b. Any site that requires a software download to a workstation may not be used unless approved by the local configuration control board or the IT Change Control Board (IT CCB) as appropriate. See 5 FAM 650 for more

information

c. Federal advisory committees have specific statutory rules that apply to such committees. Prior to using social media, chartered advisory committee members will request that their designated Federal officer seek the guidance of the Office of the Legal Adviser (L/M–Management).

5 FAM 792.2 Personal Use of Social Media

(CT:IM-110; 06-10-2010)

a. Department personnel may access and post entries to public, Internet-based social media sites, from OpenNet using their personal profile registered with a personal email address at those sites consistent with general policies on Internet use at 5 FAM 700. Personal entries must not:

   (1) Claim to represent the Department or its policies, or those of the U.S. Government, or use Department or other U.S. Government seals or logos; and

   (2) Violate ethics rules, for example, the rules prohibiting the use of public office for private gain or the disclosure of nonpublic information and the rules concerning prohibited political activity; details regarding these rules are on the L/Ethics Intranet Web site.

b. Department personnel who create and/or use nonofficial social media sites must adhere to the policies contained in 5 FAM 777 and 3 FAM 4170.

c. Department personnel who create and/or use nonofficial social media sites must not disclose information pertaining to procurement information in violation of 41 U.S.C. 423.

d. Department personnel who create and/or use non-official social media must not disclose nonpublic information, as that term is defined by 5 CFR d 2635.703(b).

e. Department personnel working abroad who create and/or use nonofficial social media cites must adhere to the policies contained in 3 FAM 4123.

f. Family members of Department personnel working abroad who create and/or use social media cites must adhere to the policies contained in 3 FAM 4125.

g. Non-U.S. citizen Department personnel and U.S. citizen Department personnel who have been hired abroad who create and/or use nonofficial social media cites must adhere to the policies contained in 3 FAM 4126.

h. For personal (nonbusiness) materials produced when using social media sites, see 5 FAH-4 H-215.6, Personal Papers, for guidance.

5 FAM 792.3 Official Use of Social Media

(CT:IM-110; 06-10-2010)

a. Department personnel may access and contribute content (both original entries and responses to entries) on social media sites in their official capacity. Department personnel should obtain supervisory approval prior to creating or contributing significant content to external social media sites or to engaging in recurring exchanges with the public.

b. Department personnel must inform the appropriate local or regional security representative of previously untested social media technologies they intend to access and of each new social media site and application that is registered in the IT assets baseline (ITAB) in accordance with 5 FAM 793.1, paragraph d.

c. To add content to social media sites, in an official capacity, personnel must use a site or email account created specifically for use in an official capacity that is separate from an account for private, personal use, except as noted in subparagraph d in this section.

d. Employees must adhere to the public information dissemination clearance requirements found in 3 FAM 4170 and 10 FAM 120 if the content is "of official concern."

e. If personal site or email accounts must be used to post content at social media sites in an official capacity, for example because the social media site does not permit multiple profiles for a single account, personnel must be mindful of the security risks related to revealing personal information.

f. Supervisors may not compel personnel either to create a personal account or personal profile at any social media site or to post personal entries at any public site. Personnel enrolled in training programs that utilize social networking programs may be required to create a personal account for the duration of the training for the purpose of instruction. Personnel may retain or delete the account or profile at their sole discretion upon the end of the training program.

5 FAM 792.4 Posting To Classified and Unclassified Social Media Sites

(CT:IM-110; 06-10-2010)

a. Users must adhere to the following policies when posting to public or personal social media sites, whether managed by the Department or another entity:

(1) Do not disclose classified information, as defined in 12 FAM 090, on public social media sites. (You can discuss classified information on classified social media platforms, in accordance with E.O. 13526, Classified National Security Information.)

(2) Do not disclose sensitive but unclassified information, as defined 12 FAM 540, on public social media sites. (You can discuss Sensitive But Unclassified (SBU) information on SBU or classified social media platforms.)

5 FAM 792.5 Counterintelligence Awareness

(CT:IM-110; 06-10-2010)

All Department personnel or other U.S. Government representatives accessing Department social media sites in any capacity must be alert to the potential targeting of users for intelligence-gathering purposes. Department personnel must remain aware of their responsibilities as outlined in 12 FAM 260. Personnel must pay particular attention to the contact reporting requirements explained in 12 FAM 262.1.

5 FAM 793 CREATING, BRANDING, AND REGISTERING AN OFFICIAL PUBLIC SOCIAL MEDIA SITE OR APPLICATION

5 FAM 793.1 Creating an Official Public Social Media Site or Application

(CT:IM-110; 06-10-2010)

a. Official Department social media sites and content must be clearly labeled and identifiable as such.

b. Department organizations may use existing commercial social media sites or use established commercial tools to develop and distribute social media applications with prior approval per 5 FAM 792.3, paragraph a.

c. Creation or use of social media sites for official purposes must have management approval at the office director level or above domestically or the public affairs officer (PAO) abroad. Such approval must include acceptance of the underlying terms of service.

d. All Department social media sites and applications must be registered in the IT assets baseline (ITAB).

5 FAM 793.2 Obtaining an Official Public Social Media Site or Application

(CT:IM-110; 06-10-2010)

a. Various procurement and IT-related laws, regulations, court decisions,

and other sources affect how social media sites or applications may be obtained or accessed. Contracting or accessing officers must ensure that a purchase or transaction represents the lowest overall cost to the U.S. Government; fully conforms to all applicable procurement laws, regulations, etc.; and contains no internal conflicts.

b. These officers must compare the proposed commercial terms of use or service to existing Departmental terms of use or terms of service agreements (or amended terms of service agreements) relating to social media and bring to the attention of the Office of the Legal Adviser (L) any significant differences between the two.

c. In addition to the above, the transaction (including applicable terms of use, etc.) must be fully in accordance with other provisions of 5 FAM 790.

5 FAM 793.3 Domain Names

(CT:IM-110; 06-10-2010)

a. The Office of Management and Budget (OMB) requires all Federal public Web sites to use the .gov, fed.us, or .mil domains in order to show they are official U.S. Government sites. Exceptions are permitted under the conditions outlined in 5 FAH-8 H-342.

b. All Department social media sites must include .gov in the domain name to the fullest extent possible.

c. In cases where customized domain names may be used, they must be requested using the Form DS-3081, Request for Registering of New or Recurring Websites.

5 FAM 793.4 Terms of Use/Terms of Service

(CT:IM-110; 06-10-2010)

a. Terms of Service refers to a contract between social media users and third-party site providers. Many third-party sites require users to agree to Terms of Service (also known as User Agreement or End User License Agreements) in order to use the service or platform. This acceptance binds the Department of State and must be performed by a direct-hire Department of State employee.

b. Terms of Use refers to an agreement between social media users and the Department. Official Department social media sites must include a Terms of Use statement that explains responsibilities of site administrators and site users, rules of behavior, privacy policies, and other terms. If the user must create an account just for the State Department social media site, agreement to the Terms of Use should be a requirement for registration. Site administrators must post the Terms of Use before

opening the site to the public.

5 FAM 793.5 Social Media Site Management

(CT:IM-110; 06-10-2010)

All social media sites require ongoing oversight to ensure proper management of the sites. In addition, the sites require sufficient maintenance and a commitment of resources. Department personnel should be aware of these commitments before requesting supervisory approval.

5 FAM 794 CONTENT AND RECORDS MANAGEMENT FOR PUBLIC SOCIAL MEDIA SITES

(CT:IM-110; 06-10-2010)

a. Content management:

(1) Content posted to social media sites by Department personnel while acting in their official capacities or used in a social media application must be relevant and accurate. When necessary, content contributors should consult with interested Department organizations regarding appropriate content to use on the social media site; and

(2) Department personnel are responsible for the content they publish in their official capacity. When Department personnel are publishing information in their official capacity, the content must:

(a) Adhere to the content and security policies in 5 FAM 776.3 and 5 FAM 777;

(b) Not promote a personal business or political point of view;

(c) Clearly indicate that an employee of the Department created the post, and in what capacity; and

(d) Adhere to host country laws. Individuals are responsible for knowing and abiding by their host country laws, as directed by local management;

(3) Information about internal Department operations and procedures is permitted on relevant Intranet sites but must not be posted on public social media sites. If Department personnel receive questions about acquisition actions or the Department's financial dealings on public social media sites, they should contact or direct the inquiry to the Bureau of Administration Acquisitions staff (A/AQM) or the Bureau of Public Affairs (PA);

(4) Copyright considerations:

(a) Copyrighted materials must be used only in accordance with current copyright laws, which typically require permission from the copyright owner. Refer to 5 FAM 490, Use of Copyrighted Material, for specific policy in this area; and

(b) Public information produced by the Department and published on social media sites or applications cannot be copyrighted and is in the public domain. No copyright insignia or statement should appear on any Department-administered social media site or application;

(5) Content monitoring and moderation:

(a) All Department organizations with a social media site must monitor user-generated content (UGC). The sponsoring organization must also determine the degree to which content will be moderated;

(b) The social media site sponsor must decide whether and how content or an application would ever be removed, by whom, and under what circumstances. This decision must be framed by records management guidance and policy in deciding whether to delete content. This information should be included in the site's Terms of Use, as described in 5 FAM 794.1. The Terms of Use must be developed prior to the site being opened to the public. The social media site sponsor should also be mindful of the general prohibition on maintaining records describing how any individual exercises rights guaranteed by the First Amendment, contained in the Privacy Act at 5 U.S.C. 552a(e)(7). The sponsor should consult with L/M before implementing any method of tracking users who consistently violate the Terms of Use; and

(c) Sponsoring organizations must monitor their social media site for clearly inappropriate content, as defined in the Terms of Use (see 5 FAM 794.4). Bureau and post management will also randomly monitor social media sites (see 5 FAM 795.2);

(6) Certain minimum standards for unacceptable content apply:

(a) No advertising or solicitation of any kind. Personnel may post links in limited circumstances, but only for informational, not promotional, purposes. When non-Federal links are provided, the social media site must include the following information: The links contained herein are for informational purposes only and do not necessarily reflect the views or endorsement of the U.S. Government or the U.S. Department of State; and

(b) Due to the open and global nature of social media sites, Department-generated Public Diplomacy content must be carefully reviewed to avoid violations of the United States Information and Educational Exchange Act of 1948, as amended (Smith-Mundt);

(7) Section 508 (Accessibility) Compliance:

(a) Consistent with 5 FAM 776.4, any content posted by Department personnel on Department-owned social media sites must be Section 508 compliant. If Department personnel post audio, video or multimedia files, the files must have transcripts, text descriptions or captioning, respectively. These should be on the same site as the file itself.

(b) Content posted by Department personnel on third-party social media sites should be Section 508 compliant if possible. As appropriate, the disclaimer for a Department page on a commercial social media site must explain that content on the site may not be compliant with Section 508, as the Department cannot control technical aspects of a social media site it does not own.

(8) Records Management:

(a) Social media site sponsors are responsible for the identification of record material and the proper archiving of that material in accordance with approved records disposition schedules. Generally there are two types of record material with most social media sites:

(b) Content records including entries, comments, blog posts, links, videos, and other social media communications; and

(c) Site management and operations records including design, policy and procedures, and other web management records;

(9) Records in social media sites must be copied or otherwise captured and maintained with related records, unless the site has a record management application that can manage the records throughout its lifecycle. Nonrecord content consisting of duplicate information which is maintained in other department recordkeeping systems (original recordkeeping copy is maintained in accordance with its records disposition schedule), and transitory records do not need to be archived and may be deleted when no longer needed.

(10) The social media site's sponsoring organization must determine whether and how long to keep the site's contents posted, or if content will be removed after a certain period of time. The decision on how long to keep a site's contents posted may be dependent on

the social media provider. If PII has been collected to register members at the site, it will not be included in any archived material. See 5 FAM 613 to determine what is considered to be PII information; and

(11) If content will be archived or removed on a periodic basis, information about what will be done with it must be included in the Terms of Use so that site members are informed.

b. Contact the Records and Archives Management staff in A/GIS/IPS/RA to develop a records disposition schedule for the records content, and site management and operations records.

5 FAM 795 PRIVACY, SECURITY, RISK ASSESSMENT, AND INCIDENT HANDLING FOR SOCIAL MEDIA USAGE

5 FAM 795.1 Privacy Requirements

(CT:IM-110; 06-10-2010)

a. Social media site managers, designers, and program offices must ensure that personally identifiable information (PII) is appropriately protected when collected, maintained and/or disseminated. (PII is defined in 5 FAM 613.)

b. Department social media sites must include in the Terms of Use a section that is equivalent in purpose to a "Web site privacy policy" as is required for all public-facing Federal Web sites and in accordance with the content criteria established in 5 FAM 772. The policy must clearly disclose any uses of persistent cookies (e.g., to create user profiles and login information or Web site usage metrics). The privacy policy should state that the social media platform's third party privacy policies apply when the visitor is using social media pages created by the Department. The privacy policy should explain that site visitors may disable persistent cookies (if used on the site) through their web browser settings. Department-developed social media applications, defined in 5 FAM 772.1, must contain a notification of how the users' profile information may or may not be used upon installing the application.

c. If PII subject to the Privacy Act is collected on a social media site, the site must include in the Terms of Use a section that is equivalent in purpose to a "Privacy Act statement" (separate from the web site privacy policy) as is required by Section (e)(3) of the Privacy Act and in accordance with the content criteria established in 5 FAM 460.

d. Users must be notified of the purpose and use of any PII collected by the social media platform, regardless of whether the PII is covered by the Privacy Act. Users must be notified whether the Department, independent of the collection by the social media platform, will collect and maintain this information in any capacity. PII must only be used in accordance with its permissible statutory purpose. Information collected for one purpose may not be used for another purpose without notice to or consent of the subject of the information.

e. The section of the Terms of Use pertaining to Web site privacy policy must include a link to the social media platform's privacy policy, with clear distinctions between the two privacy policies. It should be noted and clearly explained that users of social media are capable of posting unsolicited PII and Privacy Act-covered information on the social media site. The Department does not take responsibility for or ownership of this information. By default, the user has granted permission to the Department to see this information by joining the Department's social media site.

f. The Department must not use commercial social media sites to solicit and collect sensitive PII from individuals. Sensitive PII is a specific set of PII data elements for which loss of confidentiality, integrity, or availability could be expected to have at least a serious adverse effect on the individual based on an overall assessment of data element sensitivity, distinguishability, context of use of the PII, and the legal duty to protect the PII.

g. In accordance with 5 FAM 772, Department social media sites intended for the purpose of attracting children under the age of 13 shall comply with the applicable provisions of the Children’s Online Privacy Protection Act of 1998.

h. Social media site managers and program offices must work with the Office of Directives Management (A/GIS/DIR) to obtain approval from the Office of Management and Budget for an information collection request (ICR) when the information collected from individuals on their site triggers the requirements of the Paperwork Reduction Act (PRA). Note that the information required from an individual to register as a member of a social media site falls within the “certifications” exemption (5 CFR 1320.3(h)(1)) of the rules implementing the PRA, which allows for collections that “entail no burden other than that necessary to identify the respondent, the date, the respondent's address, and the nature of the instrument.” If the Department-sponsored page established on social media sites collects additional information from individuals who join the page or group, it may (depending on its nature and extent) trigger the requirements of the PRA. The office responsible for monitoring PRA issues is A/GIS/DIR. The ICR approval process is described at 2 FAM

1160 and 5 FAM 776.3, paragraph n.

i. If PII is being gathered on the Department social media site into an electronic collection within the scope of Section 208 of the E-Government Act, social media site managers and program offices must also conduct a Privacy Impact Assessment (PIA) in accordance with 5 FAM 611. The PIA should precisely define the scope of automation it relates to by stating the name of the involved social media site(s) and the name(s) of the specific page(s) or group(s) on each site.

5 FAM 795.2 Security Requirements, Incident Handling, and Risk Assessment

(CT:IM-110; 06-10-2010)

a. Bureau and post management, through IMOs or designated officers, will perform spot checks on Department social media sites registered in the ITAB for compliance with 5 FAM 790.

b. Social media site administrators must report and respond to security incidents if they occur, per the guidance in 5 FAM 775. Although specific corrective action may not be possible because the Department does not control commercial social media sites, all incidents should be reported to the ISSO and RSO. Concurrently, site administrators must also report security issues to the hosting social media site.

c. In the event that either PII or national security information is inadvertently lost or disclosed in an unauthorized manner, such loss or disclosure must be reported in accordance with established procedures. All such breaches should be reported immediately to the Monitoring and Incident Response Division of the Office of Computer Security (DS/CS/MIR):

   (1) Breaches involving PII will be forwarded by the Cyber Incident Response Team (DS/CS/MIR/CIRT) to the Department's Privacy Team, which will handle analysis and response consistent with OMB Memorandum M-07-16 and 5 FAM 460; and

   (2) Breaches involving national security information will be forwarded by DS-CIRT to DS/IS/APD, which will handle spillage protocol and containment in compliance with Committee on National Security Systems (CNSS) Policy No. 18.

d. Refer to 5 FAM 775 for additional information on incident handling.

e. Certification and accreditation: Department social media sites may fall below the risk impact levels that would fall below the resource thresholds for full certification and accreditation (C&A).

f. System inventory: All social media sites captured in ITAB that are rated

as low impact must be marked nonreportable for FISMA. Any others will be assessed according to current information security processes.

5 FAM 796 USING SOCIAL MEDIA ON OPENNET AND CLASSNET

(CT:IM-110; 06-10-2010)

a. The IT CCB must approve social media software installations for use in unclassified and classified networks. (See 5 FAM 861.)

b. If social media software is installed on OpenNet workstations, it must be configured for use consistent with the Federal Desktop Core Configuration and the Department's Standard Operating Environment. Social media software must not alter or interfere with Internet browser security settings.

c. For social media tools used in a classified environment, the requirements of E.O. 13526 and 5 FAM 760 concerning classified information "apply regardless of physical format and to all document types."

5 FAM 797 THROUGH 799 UNASSIGNED